UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION AT CLEVELAND

JOHN MCCARTNEY, individually and on behalf of all others similarly situated, Plaintiff, v. **NATIONSTAR d/b/a MR. COOPER** Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff, John McCartney ("Plaintiff"), individually and on behalf of all others similarly situated, and on behalf of the general public, brings this class action against Defendant, Nationstar d/b/a Mr. Cooper ("Defendant") for its failure to properly secure and safeguard Plaintiff's and Class Members' personally identifiable information ("PII") stored within Defendant's information network.

Plaintiff makes these allegations on personal information as to those allegations pertaining to themselves and their personal circumstances, and upon information and belief, based on the investigation of counsel and facts that are matters publicly known, on all other matters.

INTRODUCTION

1. Plaintiff brings this action on behalf of himself and all other individuals similarly situated ("Class Members") against Nationstar for its failure to secure and safeguard the personally identifiable information ("PII") of at least 4.3 million individuals who are either customers, mortgage brokers, or agents of the company that was maintained on Defendant's computer systems, with the intent of engaging in the misuse of the PII, including marketing and selling

Plaintiff's and Class Members' PII (the "Data Breach").[1]

2. Nationstar, headquartered in Coppell, Texas, provides mortgage loan services to the general public. In the regular course of its business, Nationstar is required to maintain reasonable and adequate security measures to secure, protect, and safeguard its customers' PII against unauthorized access and disclosures.

3. Nationstar could have prevented the Data Breach by properly vetting and monitoring the systems of its internal systems and third-party vendors.

4. Plaintiff and Class Members entrusted Nationstar with and allowed Nationstar to gather, highly sensitive information as part of obtaining financial and insurance services. They did so in confidence, and they had the legitimate expectation that Nationstar would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who legitimately needed the information and were equipped to protect it through having adequate processes in place to safeguard it.

5. Every year, millions of Americans have their most valuable PII stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to make the necessary investments to implement important and adequate security measures to protect their customers' and employees' data.

6. Defendant Nationstar required its customers to provide it with their sensitive PII and failed to protect it. Defendant had an obligation to secure its customers' PII by implementing

[1] https://incident.mrcooperinfo.com/ (last visited Nov. 3, 2023)

reasonable and appropriate data security safeguards. This was part of the bargain between Plaintiff and Class Members and Nationstar.

7. As a result of Nationstar's failure to provide reasonable and adequate data security, Plaintiff's and the Class Members' unencrypted, non-redacted PII has been exposed to unauthorized third parties. Plaintiff and the Class are now at much higher risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII stolen here and the fact that the compromised PII is already being sold on the dark web. This risk constitutes a concrete injury suffered by Plaintiff and the Class, as they no longer have control over their PII, which PII is now in the hands of third-party cybercriminals. This substantial and imminent risk of identity theft has been recognized by numerous courts as a concrete injury sufficient to establish standing.

8. Furthermore, Plaintiff and the Class, as also set forth below, will have to incur costs to pay a third-party credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

9. Plaintiff brings this action on behalf of himself and those similarly situated to seek redress for the lifetime of harm they will now face, including, but not limited to reimbursement of losses associated with identity theft and fraud, out-of-pocket costs incurred to mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, the costs of extending credit monitoring services and identity theft insurance, and injunctive relief requiring Nationstar to ensure that its third-party vendors implement and maintain reasonable data security practices going forward.

JURISDICTION AND VENUE

10. Subject matter jurisdiction arises under 28 U.S.C. § 1332(d). This case is brought as a class action because at least one Class Member is of diverse citizenship from Defendant, there are 100 or more Class Members nationwide, and the aggregate amount in controversy exceeds $5,000,000. The Court has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(3) because the Court has personal jurisdiction over Defendant, a substantial portion of the alleged wrongdoing occurred in this District and the state of Ohio, and Defendant has sufficient contacts with this District and the state of Ohio.

12. Venue is proper in the Northern District of Ohio pursuant to 28 U.S.C. § 1391(b)(2) because a substantial number of the events or omissions giving rise to the claims at issue in this Complaint arose in this District. The Plaintiff resides in Cuyahoga County; thus, the Northern Division is proper.

THE PARTIES

Plaintiff John McCartney

13. Plaintiff, John McCartney ("Mr. McCartney"), is a resident of Ohio, who has a mortgage loan serviced by Nationstar on his home in Strongsville, Cuyahoga County, Ohio.

14. In the course of using Nationstar's services, Mr. McCartney was required to provide his PII to Defendant, including his name, social security number, date of birth, and address.

15. As a result, Mr. McCartney's information was among the data accessed by an unauthorized third party in the Data Breach.

16. At all times herein relevant, Mr. McCartney is and was a member of the Class.

17. As a result of the Data Breach, Mr. McCartney was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time

spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring his accounts with heightened scrutiny, time spent dealing with the consequences of account fraud, time spent filing a police report, and time spent seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach.

18. Mr. McCartney was also injured by the material risk to future harm he suffers based on the Defendant's breach; this risk is imminent and substantial because Mr. McCartney's data has been exposed in the breach, the data involved is highly sensitive and presents a high risk of identity theft or fraud.

19. Mr. McCartney suffered actual injury in the form of damages to and diminution in the value of his PII that he entrusted to Defendant, and which was compromised in and as a result of the Data Breach.

20. Mr. McCartney, as a result of the Data Breach, has increased anxiety about his loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling his PII.

21. Mr. McCartney has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

22. Mr. McCartney has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in the Defendant's possession, is protected and safeguarded from future breaches.

Defendant Nationstar d/b/a Mr. Cooper

23. Defendant Nationstar Financial, Inc. is a Delaware limited liability company with

its principal place of business at 8950 Cypress Waters Blvd, Coppell, Texas.

24. Nationstar advertises that it provides financial and mortgage services to help its customers "keep the dream of home ownership alive" by making the homeownership journey "less worrisome and more rewarding every step of the way."[2]

25. Nationstar describes itself to be one of the largest home loan servicers in the country serving at least 3.8 million homeowners.

26. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

27. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

28. Plaintiff brings this action pursuant to the provisions of Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of himself and the following Classes:

Nationwide Class

> All persons residing in the United States who are current or former customers of Nationstar or any Nationstar affiliate, parent, or subsidiary, and had their PII compromised by an unknown third-party cybercriminal as a result of the Data Breach.

In addition, Plaintiff brings this action on behalf of the following proposed Ohio Subclass defined as follows:

[2] https://www.mrcooper.com/about-us/overview (Last visited November 3, 2023).

Ohio Subclass

All persons residing in the State of Ohio who are current or former customers of Nationstar or any Nationstar affiliate, parent, or subsidiary, and had their PII compromised as a result of the Data Breach.

29. Both the proposed Nationwide Class and the proposed Subclasses will be collectively referred to as the Class, except where it is necessary to differentiate them.

30. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

31. Plaintiff reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

32. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

33. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class (which Plaintiffs are informed and believe, and on that basis, allege that the total number of persons exceeds 4.1 million of individuals) are so numerous that joinder of all members is impractical, if not impossible.

34. Commonality: Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether the Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. How and when Defendant actually learned of the Data Breach;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class Members;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

35. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

36. Adequacy of Representation: Plaintiff is an adequate representative of the Class in that the Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case, and has retained competent counsel who is experienced in conducting litigation of this nature.

37. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the class in its entirety. Plaintiff anticipates no management difficulties in this litigation.

38. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought

or be required to be brought by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

39. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

40. This class action is also appropriate for certification because the Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

41. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

42. Unless a Class-wide injunction is issued, Defendant may continue failing to properly secure the PII of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

43. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

Defendant's Data Breach

44. On November 2, 2023, Mr. Cooper, on behalf of Nationstar, issued a Data Breach

Notice (the "Notice") to notify its customers that an unauthorized party accessed Nationstar systems on or about October 31, 2023, downloading highly sensitive PII of at least 4.1 million Nationstar customers and brokers or agents stored on its servers, including Social Security numbers, first and last names, dates of birth, and addresses.

45. Additionally, Nationstar posted a Security Event Notice ("Security Notice") on its website that vaguely discussed the Data Breach and even vaguer steps taken to ensure a Data Breach of this kind does not happen again - "We value our customers and take their data privacy very seriously. Following detection of the incident, we immediately initiated response protocols, including deploying containment measures to protect systems and customer data, as well as shut down certain systems as a precautionary measure."

46. Absent from the Notice and Security Notice are any details regarding how the Data Breach happened, what Nationstar did in response, or whether Nationstar has taken action to remediate the root cause of the Data Breach.

Defendant Collected/Stored Class Members' PII

47. Defendant acquired, collected, stored, and assured reasonable security over Plaintiff's and Class Members' PII.

48. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PII.

49. Defendant, in turn, stored that information in the part of Defendant's computer and information system that was ultimately affected by the Data Breach.

50. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant

assumed legal and equitable duties to protect that PII and knew or should have known that it was thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

51. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

52. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized use of this information.

53. Defendant in its own privacy policy provides written assurances to the Plaintiff and Class Members that their PII is secure:

> "Keeping financial information is one of our most important responsibilities. Only those persons who need it to perform their job responsibilities are authorized to access your information. We take commercially reasonable precautions to protect your information and limit disclosure by maintaining physical, electronic and procedural safeguards."[3]

> "To protect your personal information from unauthorized access and use, we use
> security measures that comply with federal law. These measures include computer
> safeguards and secured files and buildings. We also contractually require third parties doing business with us to comply with all privacy and security laws."[4]

54. Defendant could have prevented the Data Breach, which began no later than October 31, 2023, by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PII.

---

[3] https://www.mrcooper.com/privacy

[4] https://www.mrcooper.com/reference_documents/apollo_mr_cooper/MrCooper_Privacy_Notice.pdf (Last visited November 3, 2023).

55. The Defendant's negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by its previous experience with data breaches, repeated warnings, and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

56. Yet, despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

57. Defendant's failure to adequately secure Plaintiff's and Class Members' sensitive PII breaches duties it owes Plaintiff and Class Members under statutory and common law. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

58. In 2022, 1,802 data breaches occurred, resulting in over 422,000,000 sensitive records being exposed.[5] The over 422,000,000 records being exposed in 2022 represents a substantial increase from 2021 when 293,927,708 sensitive records were exposed in 1,862 data breaches.[6]

59. In light of recent high profile data breaches at other industry leading companies,

[5] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited Oct. 4, 2023)
[6] *Id.; see also* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (https://notified.idtheftcenter.org/s/), at 6. (last visited Oct. 3, 2023)

including MOVEIt (17.5 Million Records, June 2023), LastPass/GoTo Technologies (30 Million Records, August 2022), Neopets (69 Million Records, July 2022), WhatsApp (500 million records, November 2022), Twitter (5.4 Million records, July 2022), Cash App (8.2 Million Users, April 2022), LinkedIn (700 Million Records, April 2021), Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

60. Moreover, the Defendant was, or should have been, aware of the foreseeable risk of a cyberattack, like the one it experienced.

61. The Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."[7]

62. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

63. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its

[7] The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

64. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, networks, and personnel policies and procedures to ensure that the PII was adequately secured and protected.

65. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

66. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

67. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

68. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

69. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

70. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

71. PII are valuable commodities for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

72. Numerous sources cite dark web pricing for stolen identity credentials; for example, , personal information is sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] Criminals also can purchase access to entire sets of information obtained from company data breaches for prices ranging from $900 to $4,500.[9]

73. Social Security numbers are among the worst kinds of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

74. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[10]

75. In addition, it is no easy task to change or cancel a stolen Social Security number.

---

[8] Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-onthe-dark-web-how-much-it-costs/ (Last visited November 3, 2023).
[9] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark (Last visited November 3, 2023).
[10] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (Last visited November 3, 2023).

An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.[11]

76. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

77. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, in that situation, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, birthdate, and Social Security number.

78. This data commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[12]

79. Identity thieves can use PII, such as that of Plaintiff's and Class Members, which

[11] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-shackers-has-millionsworrying-about-identity-theft (Last visited November 3, 2023).

[12] Time Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10xprice-of-stolen-credit-card-numbers.html (Last visited November 3, 2023)

Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

80. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[13]

81. Here, Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

82. The Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Therefore, its failure to do so is intentional, willful, reckless and/or grossly negligent.

83. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i)

---

[13] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed September 22, 2023).

intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

Common Injuries & Damages Suffered by the Plaintiff and Putative Class

84. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is present and continuing, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

85. The Plaintiff and Class Members are at a heightened risk of identity theft for years to come. The link between a data breach and the risk of identity theft is simple and well-established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the

information to commit a variety of identity theft-related crimes discussed below.

86. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

87. Plaintiff and Class Members have spent and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach.

88. These efforts are consistent with the U.S. Government Accountability Office report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[14]

89. These efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit,

[14] See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report"). (last visited Oct. 3, 2023)

and correcting their credit reports.[15]

90. The value of the PII of the Plaintiff and Class Members is valuable.[16] Its value is axiomatic, considering the value of Big Data in corporate America and the criminal consequences of cyber thefts, which include significant prison sentences and fines. Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has a considerable market value.

91. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[17]

92. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the PII has been lost, thereby causing additional loss of value.

93. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

94. There is a strong probability that entire batches of stolen information have been

---

[15] *Id*.

[16] See, e.g., Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted) (Last visited November 3, 2023).

[17] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited November 3, 2023).

placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes ——e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

95. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. And fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

96. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

CLAIMS FOR RELIEF

COUNT ONE

Negligence

(On behalf of the Plaintiff and the Class)

97. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

98. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and

storing the PII of Plaintiff and Class Members in its computer systems and on its networks.

99. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession;

b. to protect Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

100. Defendant knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

101. Defendant knew or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security.

102. Defendant knew about numerous, well-publicized data breaches.

103. Defendant knew or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

104. Only Defendant was in the position to ensure that its systems and protocols were

sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

105. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII.

106. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

107. Plaintiff's and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions.

108. Moreover, only Defendant had the ability to protect its systems and the PII it stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

109. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiff, and/or the remaining Class Members.

110. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly

disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees not to store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

111. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

112. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages.

113. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure

obligations to Plaintiff and Class Members.

114. Further, through its failure to provide clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

115. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

116. Plaintiff's and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

117. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

118. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

119. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from

embarrassment and identity theft;; (vi) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

120. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

121. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT TWO
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

122. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

123. Through its course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

124. Defendant required Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining Defendant's services.

125. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices.

126. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

127. As a condition of being direct consumers of Defendant, Plaintiff and Class Members provided and entrusted their PII to Defendant.

128. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

129. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII.

130. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

131. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide accurate notice to them that their PII was compromised as a result of the Data Breach.

132. As a direct and proximate result of Defendant's above-described breach of implied

contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

133. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

134. Additionally, as a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT THREE
Breach of Fiduciary Duty
(On behalf of the Plaintiff and the Class)

135. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

136. Defendant benefited from receiving Plaintiff's and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

137. In providing their PII to Defendant for the purpose of engaging in business transactions with Defendant, Plaintiff and the Class Members placed a special trust in Defendant to securely maintain and protect their PII from unauthorized access and distribution.

138. By requesting and accepting the Plaintiff's and the Class Members' PII, Defendant knew that the Plaintiff and Class Members placed a special trust in Defendant to securely maintain and protect their PII from unauthorized access and distribution.

139. Based upon the relative knowledge and skill necessary for Defendant to secure the PII of Plaintiff and Class Members, Defendant's relationship with Plaintiff and Class Members went beyond a common business relationship and was in fact a fiduciary relationship.

140. The Plaintiff and Class Members were at all times ordinary consumers who lacked the skills and knowledge related to the security needs necessary for Defendant to maintain when it received the PII. As such, Defendant owed a fiduciary duty to Plaintiff and Class Members to take all steps necessary to secure and protect the PII of Plaintiff and Class Members in compliance with all industry standards and in compliance with all applicable state and federal laws and regulations.

141. Based on the allegations above, *supra*, Defendant breached its fiduciary duty by failing to maintain the safety and security of the PII of Plaintiff and Class Members at all times and allowing the Breach to occur.

142. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary

loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

143. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

144. Additionally, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

145. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and Class Members are entitled to an award of actual damages and an award of punitive damages in an amount to be determined at trial.

COUNT FOUR
Invasion of Privacy
(Intrusion Upon Seclusion)
(On behalf of Plaintiffs and the Class)

146. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

147. The Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

148. As a result of Defendant's conduct, publicity was given to the Private Information of Plaintiff and Class Members which necessarily includes matters concerning their private life such as their PII.

149. The Private Information of the Plaintiff and Class Members is not of legitimate public concern and should remain private.

150. By knowingly failing to keep the Private Information of the Plaintiff and Class Members safe, and by knowingly misusing said information, Defendant negligently, recklessly, and intentionally invaded the privacy of the Plaintiff and Class Members by intruding into the private affairs of the Plaintiff and Class Members, without approval, in a manner that would be highly offensive and objectionable to a person of ordinary sensibilities.

151. Defendant knew that an ordinary person in the position of Plaintiff or Class Members would consider Defendant's negligent, reckless, and intentional actions highly offensive and objectionable.

152. Such an intrusion into the private affairs of the Plaintiff and Class Members is likely to cause outrage, shame, and mental suffering because the Private Information disclosed includes financial information and sensitive personal information like Social Security Numbers that allow third parties to commit fraud and identity theft.

153. Defendant invaded the right to privacy of the Plaintiff and the Class Members and intruded into the private lives of the Plaintiff and Class members by negligently, recklessly, and intentionally misusing their Private Information without their informed, voluntary, affirmative, and clear consent.

154. Defendant intentionally concealed from Plaintiff and Class Members an incident

that misused their Private Information without their informed, voluntary, affirmative, and clear consent.

155. As a proximate result of such intentional misuse, the reasonable expectations of privacy that the Plaintiff and Class Members have in their Private Information was unduly frustrated and thwarted.

156. Defendant's conduct amounts to a substantial and serious invasion of the protected privacy concerns of the Plaintiff and Class Members causing anguish and suffering such that a person with ordinary sensibilities would consider Defendant's intentional actions or inaction highly offensive and objectionable.

157. In failing to protect Plaintiff's and Class Members' Private Information, and in negligently, recklessly, and intentionally misusing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of the rights of the Plaintiff and Class Members to have such information kept secure, confidential, and private.

158. As a direct and proximate result of Defendant's invasion of privacy, the Plaintiff and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in

the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information of the Plaintiff and Class Members.

159. The Plaintiff and Class Members are entitled to compensatory, consequential, punitive, and nominal damages suffered as a result of the Data Breach.

160. The Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VI
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiffs and the Class)

161. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

162. As described above, when Plaintiff and the Class Members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiffs' and Class Members' PII and to timely detect and notify them in the event of a data breach.

163. These exchanges constituted an agreement between the parties: Plaintiff and Class Members were required to provide their PII in exchange for products and services provided by Defendant, as well as an implied covenant by Defendant to protect Plaintiff's and Class Members' PII in its possession.

164. It was clear by these exchanges that the parties intended to enter into an agreement.

165. Plaintiff and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of certain products and services. Conversely, Defendant presumably would not have taken Plaintiff's and Class Members' PII if it did not intend to provide Plaintiffs and Class Members with the products and services it was offering.

166. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class Members in its possession was only used to provide the agreed- upon products and services.

167. Plaintiff and Class Members therefore did not receive the benefit of the bargain with Defendant, because they provided their PII in exchange for Nationstar's implied agreement to keep it safe and secure.

168. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

169. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' PII; storing the PII of former customers, despite any valid purpose for the storage thereof having ceased upon the termination of the business relationship with those individuals; and failing to disclose to Plaintiff and Class Members at the time they provided their PII to it that Defendant's data security systems failed to meet applicable legal and industry standards.

170. Plaintiff and Class Members did all or substantially all the significant things that

the contract required them to do.

171. Likewise, all conditions required for the Defendant's performance were met.

172. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class Members' rights to receive the full benefit of their contracts.

173. Plaintiff and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

174. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

175. Plaintiff and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and each member of the proposed Class, respectfully requests that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

A. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

B. For an award of damages, including actual, nominal, and consequential damages,

as allowed by law in an amount to be determined;

C. That the Court enjoin Defendant, ordering them to cease from unlawful activities;

D. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

E. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

v. requiring Defendant to engage independent third-party security auditors and

internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

vi. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

x. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xi. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

xii. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

F. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

G. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

H. For all other Orders, findings, and determinations identified and sought in this Complaint.

Respectfully submitted:

/s/ Brian D. Flick
Marc E. Dann (0039425)
Brian D. Flick (0081605)
Andrew M. Engel (0047371)
DannLaw
15000 Madison Ave.
Lakewood, OH 44107
(216) 373-0539
(216) 373-0536 – fax
notices@dannlaw.com

Attorneys for Plaintiff John McCartney and the putative class

JURY DEMAND

Plaintiff, individually and on behalf of the Plaintiff, Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

/s/ Brian D. Flick
Marc E. Dann (0039425)
Brian D. Flick (0081605)
Andrew M. Engel (0047371)
DannLaw
Attorneys for Plaintiff John McCartney and the putative class